

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Applicants: Takehiko NAKANO et al.  
International Application No.: PCT/JP2004/003327  
International Filing Date: March 12, 2004  
For: DEVICE-TO-DEVICE AUTHENTICATION SYSTEM,  
DEVICE-TO-DEVICE AUTHENTICATION METHOD,  
COMMUNICATION APPARATUS, AND COMPUTER  
PROGRAM

745 Fifth Avenue  
New York, NY 10151

**EXPRESS MAIL**

Mailing Label Number: EV206809689US

Date of Deposit: January 11, 2005

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop PCT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Adam Ahmed  
(Typed or printed name of person mailing paper or fee)

[Signature]  
(Signature of person mailing paper or fee)

**CLAIM OF PRIORITY UNDER 37 C.F.R. § 1.78(a)(2)**

Mail Stop PCT  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Pursuant to 35 U.S.C. 119, this application is entitled to a claim of priority to Japan  
Application No. 2003-132904 filed 12 May 2003.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP  
Attorneys for Applicants

By: [Signature]  
William S. Frommer  
Reg. No. 25,506  
Tel. (212) 588-0800

10/520974

JP2004/003327

Rec'd PCT/PTO 11 JAN 2005

日本国特許庁  
JAPAN PATENT OFFICE

12.3.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application: 2003年 5月12日

出願番号  
Application Number: 特願2003-132904  
[ST. 10/C]: [JP2003-132904]

出願人  
Applicant(s): ソニー株式会社

REC'D 29 APR 2004

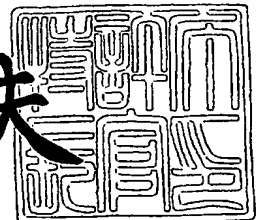
WIPO PCT

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 4月16日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



出証番号 出証特2004-3032132

【書類名】 特許願

【整理番号】 0390410005

【提出日】 平成15年 5月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 中野 雄彦

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 高林 和彦

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 本田 康晃

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 五十嵐 卓也

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

## 【選任した代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

## 【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

## 【手数料の表示】

【予納台帳番号】 048747

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項1】

ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証システムであって、

前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離するローカル環境管理手段と、  
を具備することを特徴とする機器間認証システム。

【請求項2】

一方の機器は前記ルータ経由で前記外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器は前記ホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

前記ローカル環境管理手段により前記ホーム・ネットワークを前記外部ネットワークから隔離した状態で、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、  
ことを特徴とする請求項1に記載の機器間認証システム。

【請求項3】

前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能であり、

前記ローカル環境管理手段は、ホーム・サーバ毎にクライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断する、  
ことを特徴とする請求項1に記載の機器間認証システム。

【請求項4】

クライアントは、同じホーム・ネットワーク上の2台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項3に記載の機器間認証システム。

#### 【請求項5】

クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、その以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項3に記載の機器間認証システム。

#### 【請求項6】

前記ローカル環境管理手段は、前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワーク間の経路を再開させる、

ことを特徴とする請求項1に記載の機器間認証システム。

#### 【請求項7】

ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証方法であって、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離する、

ことを特徴とする機器間認証方法。

#### 【請求項8】

一方の機器は前記ルータ経由で外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントであり、

前記ホーム・ネットワークを前記外部ネットワークから隔離した状態で、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう、

ことを特徴とする請求項7に記載の機器間認証方法。

【請求項9】

前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能であり

ホーム・サーバ毎に、クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断する、

ことを特徴とする請求項7に記載の機器間認証方法。

【請求項10】

クライアントは、同じホーム・ネットワーク上の2台以上のホーム・サーバからコンテンツの提供及び／又はコンテンツに関するライセンスの発行を受けることができる、

ことを特徴とする請求項9に記載の機器間認証方法。

【請求項11】

クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、その以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となる、

ことを特徴とする請求項9に記載の機器間認証方法。

【請求項12】

前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワーク間の経路を再開させる、

ことを特徴とする請求項7に記載の機器間認証方法。

【請求項13】

ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で動作する通信機器であって、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記ホーム・ネットワークを前記外部ネットワークから遮断するこ

とを要求するローカル環境管理手段を備える、  
ことを特徴とする通信機器。

【請求項14】

ホーム・ネットワーク上でコンテンツを提供するホーム・サーバとして動作し

、  
前記ローカル環境管理手段は、クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう際に、前記ホーム・ネットワークを前記外部ネットワークから遮断することを要求する、  
ことを特徴とする請求項13に記載の通信機器。

【請求項15】

前記ローカル環境管理手段は、クライアントとのローカル通信の終了後、前記ホーム・ネットワークと前記外部ネットワークとの接続を再開することを要求する、  
ことを特徴とする請求項14に記載の通信機器。

【請求項16】

ホーム・ネットワークと外部ネットワークを相互接続する通信機器であって、  
前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する  
経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離する制御手段と、  
を具備することを特徴とする通信機器。

【請求項17】

前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの遮断要求に応じて前記ホーム・ネットワークを前記外部ネットワークから隔離する、  
ことを特徴とする請求項16に記載の通信機器。

【請求項18】

前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム

・サーバからの再開要求に応じて、遮断中の前記ホーム・ネットワークと前記外部ネットワークの接続を再開する、  
ことを特徴とする請求項 16 に記載の通信機器。

**【請求項 19】**

前記制御手段は、前記ホーム・ネットワーク上でコンテンツを提供するホーム・サーバからの遮断要求に応じて前記ホーム・ネットワークを前記外部ネットワークから隔離した後、所定のタイミングで前記ホーム・ネットワークと前記外部ネットワークの接続を再開する、  
ことを特徴とする請求項 16 に記載の通信機器。

**【請求項 20】**

前記ホーム・ネットワークと前記外部ネットワークを遮断中に、前記外部ネットワークと通信する手段と、

前記ホーム・ネットワークと前記外部ネットワークを遮断中に、前記外部ネットワーク上の所定のサーバにアクセスして、前記ホーム・ネットワークと前記外部ネットワークとの経路が遮断していることを確認する手段と、  
をさらに備えることを特徴とする請求項 16 に記載の通信機器。

**【請求項 21】**

ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングを取得するステップと、

該タイミングにおいて、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離せしめるステップと、

を具備することを特徴とするコンピュータ・プログラム。

**【発明の詳細な説明】**

**【0001】**

**【発明の属する技術分野】**

本発明は、ネットワークなどによって配信される音楽データや画像データ、電子出版物などのデジタル・データや動画像などコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに係り、特に、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに関する。

#### 【0002】

さらに詳しくは、本発明は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上で、著作権法で認められる私的使用の範囲内でコンテンツの利用を管理する機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに係り、特に、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように管理する機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムに関する。

#### 【0003】

##### 【従来の技術】

近年のインターネットの普及により、コンピュータ・ファイルを始めとした各種のデジタル・コンテンツをネットワーク配信することが盛んに行なわれている。また、広帯域通信網（xDSL（x Digital Subscriber Line）、CATV（Cable TV）、無線ネットワークなど）の普及により、音楽データや画像データ、電子出版物などのデジタル・データや、さらには動画像などリッチ・コンテンツの配信もユーザにストレスなく伝送できるような仕組みが整いつつある。

#### 【0004】

一方、配信されるコンテンツはデジタル・データであり、コピーや改竄などの不正な操作を比較的容易に行なうことができる。また、現在これらのコンテンツのコピーや改竄などの不正行為は頻繁に行なわれており、これがデジタル・コンテンツ・ベンダの利益を阻害する主要な要因となっている。この結果、コンテンツの値段も高くしなければならなくなり、普及の障壁となるという悪循環が起こ

っている。

#### 【0005】

例えば、最近では一般家庭内にもコンピュータやネットワークなどの技術が深く浸透してきている。家庭内のパーソナル・コンピュータやPDA (Personal Digital Assistants) などの情報機器、さらにはテレビ受像機やビデオ再生装置などの各種の情報家電がホーム・ネットワーク経由で相互接続されている。また、このようなホーム・ネットワークは、多くの場合、ルータ経由でインターネットを始めとする外部の広域ネットワークに相互接続されている。そして、インターネット上のサーバから正当に取得されたコンテンツは、ホーム・ネットワーク上のサーバ（以下、「ホーム・サーバ」とも呼ぶ）に蓄積された後、家庭内の他の端末（クライアント）へホーム・ネットワーク経由で配信される。

#### 【0006】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている（著作権法第30条を参照のこと）。

#### 【0007】

この私的使用の範囲を上述したホーム・ネットワークにおいて適用した場合、ホーム・ネットワークに接続されているクライアント端末は、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される（勿論、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある）。

#### 【0008】

しかしながら、ホーム・ネットワーク上にログインしたクライアント端末が私的使用の範囲にあるかどうかを識別することは、現状の技術では困難である。

#### 【0009】

例えば、ホーム・ネットワークはルータを介して外部のネットワークとIPプロトコル・ベースで相互接続されていることから、ホーム・サーバにとってはアクセスしてきたクライアントが実際にどこにいるのかは不明である。外部（遠隔）からのアクセスに対しホーム・サーバがコンテンツを提供してしまうと、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しい。この結果、コンテンツ製作者は創作意欲を失いかねない。

#### 【0010】

また、ホーム・サーバがホーム・ネットワーク内のクライアント端末に対して一様にコンテンツの利用を許可した場合、同じクライアント端末が時間差をおいて複数のホーム・ネットワークに跨ってログインすることにより、ほぼ無尽蔵にコンテンツを利用することが可能となってしまう。

#### 【0011】

他方、クライアント端末に対して厳しい制限を課してしまうと、ユーザは、本来著作権法上で認められている私的使用を確保することができなくなってしまう。この結果、ユーザがコンテンツを十分に享受することができず、ホーム・サーバやコンテンツ配信サービスの利用が進まないために、コンテンツ事業の発展自体を阻害しかねない。

#### 【0012】

例えば、著作物を正規に購入した利用者に自由利用が認められているということに鑑み、利用者がネットワーク上での情報を複製して利用するにあたって、コンテンツの権利保持者の理解が得られ易い方法に関する提案がなされている（例えば、特許文献1を参照のこと）。しかしながら、これは利用者を情報の利用権保持者との関係レベルによって分類し、関係レベル毎に異なる配信方法で情報を配信するというもので、ネットワーク上のどこまでが私的使用の範囲にあるかを識別するものではない。

#### 【0013】

ホーム・ネットワークを構成するプロトコルとして、例えばUPnP（Universal Plug and Play）が知られている。UPnPによれば、複雑な操作を伴うことなく容易にネットワークを構築することが可能であり

、ネットワーク接続された機器間では困難な操作や設定を伴うことなくコンテンツ提供サービスを行なうことが可能となる。また、UPnPは、オペレーティング・システム（OS）に非依存であり、容易に機器の追加ができるという利点を持つ。

#### 【0014】

UPnPでは、ネットワーク接続された機器間で、XML（eXtended Markup Language）形式で記述された定義ファイルを交換して相互認証を行なう。UPnPの処理の概要は以下の通りである。

#### 【0015】

- (1) アドレッシング処理：IPアドレスなどの自己のデバイスIDを取得する
- (2) ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する
- (3) サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

#### 【0016】

このような処理手順を行なうことで、ネットワーク接続された機器を適用したサービスの提供並びに受領が可能となる。新たにネットワークに接続される機器は、アドレッシング処理によりデバイスIDを取得し、ディスカバリ処理によりネットワーク上の他のデバイスについての情報を取得し、サービス要求が可能となる。

#### 【0017】

ホーム・サーバに格納されたコンテンツは、ホーム・ネットワーク上の他の機器からアクセス可能となる。例えば、UPnP接続を実行した機器によってコンテンツを取得することが可能である。コンテンツが映像データや音声データの場合、ネットワーク接続機器として、TVやプレーヤなどを接続すれば、映画や音楽を視聴することができる。

#### 【0018】

しかし、ホーム・ネットワーク内の機器、例えばホーム・サーバには私的なコンテンツや有料コンテンツなど著作権管理を要求されるコンテンツが格納されて

いることから、不正アクセスの対策を考慮する必要がある。

#### 【0019】

コンテンツの利用権（ライセンス）を有するユーザの機器によるアクセスは許容されて当然である。しかしながら、ホーム・ルータ経由で外部ネットワークに相互接続されているホーム・ネットワーク環境では、ライセンスを持たないユーザがホーム・ネットワークに入り込むことも可能である。

#### 【0020】

不正アクセスを排除するため、例えば、ホーム・サーバにアクセスを許容するクライアントのリストを保持させ、クライアントからホーム・サーバへのアクセス要求が行なわれる度に、リストとの照合処理を実行して、不正アクセスを排除することができる。

#### 【0021】

例えば、各通信機器に固有の物理アドレスであるMAC（Media Access Control）アドレスを用いてアクセス許容機器リストとして設定するMACアドレス・フィルタリングが知られている。すなわち、ホーム・ネットワークのような内部ネットワークと外部ネットワークとを隔離するルータ又はゲートウェイにアクセスを許容する各機器のMACアドレスを登録しておき、受信したパケットに付されているMACアドレスと登録されたMACアドレスとを照合し、未登録のMACアドレスを持つ機器からのアクセスを拒否する（例えば、特許文献2を参照のこと）。

#### 【0022】

しかしながら、アクセス許容機器リストを構築するためには、内部ネットワークに接続されるすべての機器のMACアドレスを調べる必要があり、また、取得したすべてのMACアドレスを入力してリストを作成する手間が必要である。また、ホーム・ネットワークにおいては、接続される機器が比較的頻繁に変更され、かかる変更の度にアクセス許容機器リストを修正しなければならない。

#### 【0023】

#### 【特許文献1】

特開2002-73861号公報

**【特許文献 2】**

特開平 1 0 - 2 7 1 1 5 4 号公報

**【0 0 2 4】****【発明が解決しようとする課題】**

本発明の目的は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上でのコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することにある。

**【0 0 2 5】**

本発明のさらなる目的は、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することにある。

**【0 0 2 6】****【課題を解決するための手段及び作用】**

本発明は、上記課題を参酌してなされたものであり、その第 1 の側面は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証する機器間認証システムであって、

前記外部ネットワークと前記ホーム・ネットワーク間の経路を接続・遮断する経路遮断手段と、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングにおいて、前記経路遮断手段を作動させて前記ホーム・ネットワークを前記外部ネットワークから隔離して、前記ホーム・ネットワーク内でのローカル通信を実現するローカル環境管理手段と、

を具備することを特徴とする機器間認証システムである。

**【0 0 2 7】**

但し、ここで言う「システム」とは、複数の装置（又は特定の機能を実現する機能モジュール）が論理的に集合した物のことを言い、各装置や機能モジュール

が単一の筐体内にあるか否かは特に問わない。

#### 【0028】

ここで、一方の機器は前記ルータ経由で外部ネットワークからコンテンツを正当に取得するホーム・サーバであり、他方の機器はホーム・サーバに対してコンテンツを要求し利用するクライアントである。そして、双方の機器が同じホーム・ネットワーク上に存在することが確認されたことに応じて、前記ホーム・サーバは前記クライアントに対しコンテンツの提供及び／又はコンテンツに関するライセンスの発行を行なう。

#### 【0029】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用することを目的としてコンテンツを複製することが許されている。

#### 【0030】

前記ホーム・ネットワーク上には2台以上のホーム・サーバを設置可能である。このような場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、それぞれ独自にこれらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。さらに、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

#### 【0031】

この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当である。

#### 【0032】

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、時間差をおいて、複数のホーム・ネットワークに跨って複数のホ

ーム・サーバのグループに所属することまでは認めるべきでない。別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。

#### 【0033】

したがって、クライアントは、同じホーム・ネットワーク上の複数のホーム・サーバから取得したコンテンツを利用可能であるが、別のホーム・ネットワーク上のホーム・サーバに接続した時点で、その以外のホーム・ネットワーク上のホーム・サーバから取得したコンテンツを利用不能となるようにする。

#### 【0034】

現状のネットワーク・プロトコルでは、ネットワーク経由で相互接続されている機器同士が真正すなわち個人的又は家庭の範囲内でコンテンツを私的使用できるかどうかを識別する仕組みは提供されていない。そこで、本発明では、ホーム・ネットワークと外部ネットワークの経路を一時的に遮断することにより、その期間において通信し合える機器が同じホーム・ネットワーク上に存在することを保証するようにした。

#### 【0035】

本発明によれば、ホーム・ネットワークと外部ネットワークの経路を遮断したり接続したりする制御機構を例えばホーム・ルータに装備する。そして、ホーム・サーバがクライアント端末をメンバー登録したり、コンテンツの提供やそのライセンスの発行を行ったりするなど、ローカル環境下での通信であることを保証しなければならないタイミングにおいて、ホーム・ネットワークと外部ネットワークとの経路を遮断する。この結果、ホーム・サーバがローカル通信を行ない、ローカル環境下に存在するクライアント端末のみがホーム・サーバ上に蓄積されているコンテンツを利用することができるようになる。

#### 【0036】

前記ホーム・ネットワーク上でのローカル通信が完了後、又はローカル通信を開始してから所定時間経過後に、前記ホーム・ネットワークと前記外部ネットワ

ーク間の経路を再開させればよい。

#### 【0037】

また、本発明の第2の側面は、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上の機器を認証するための処理をコンピュータ・システム上で実行するようにコンピュータ可読形式で記述されたコンピュータ・プログラムであって、

前記ホーム・ネットワーク上の機器間で通信を行なうことを保証するタイミングを取得するステップと、

該タイミングにおいて、前記外部ネットワークと前記ホーム・ネットワーク間の経路を一時的に遮断して前記ホーム・ネットワークを前記外部ネットワークから隔離せしめるステップと、

を具備することを特徴とするコンピュータ・プログラムである。

#### 【0038】

本発明の第2の側面に係るコンピュータ・プログラムは、コンピュータ・システム上で所定の処理を実現するようにコンピュータ可読形式で記述されたコンピュータ・プログラムを定義したものである。換言すれば、本発明の第2の側面に係るコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の第1の側面に係る機器間認証システムと同様の作用効果を得ることができる。

#### 【0039】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施形態や添付する図面に基づくより詳細な説明によって明らかになるであろう。

#### 【0040】

##### 【発明の実施の形態】

以下、図面を参照しながら本発明の実施形態について詳解する。

#### 【0041】

著作権法の下、著作物としてのコンテンツは無断の複製や改竄などの不正使用から保護を受ける。一方、著作物の正当な利用者においては、私的な使用、すなわち個人的に又は家庭内その他これに順ずる限られた範囲内において使用するこ

とを目的としてコンテンツを複製することが許されている（著作権法第30条を参照のこと）。

#### 【0042】

本発明者らは、ホーム・ネットワーク内（以下、「ローカル環境」とも呼ぶ）のクライアント端末は、私的な使用の範囲内にあるという前提に立ち、ローカル環境下のクライアントに限り、ホーム・サーバ上に蓄積されているコンテンツを利用することができるというシステムを提案する。

#### 【0043】

ここで、ローカル環境の定義について説明しておく。

#### 【0044】

図1には、ホーム・ネットワークの基本構成を模式的に示している。同図に示すように、家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどの外部ネットワークに接続されている。

#### 【0045】

ホーム・ネットワーク上には、ホーム・サーバと、1以上のクライアント端末が存在する。ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。勿論、ホーム・サーバは、パッケージ・メディアや放送受信など、ネットワーク以外の手段により、コンテンツを取得することができる。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用する。

#### 【0046】

ホーム・ネットワークに接続されているクライアント端末は、ローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定される。したがって、ホーム・サーバにおいて正当に取得されているコンテンツは、ホーム・ネットワーク上のクライアント端末は自由に使用することが相当であると思料される。

#### 【0047】

そこで、ホーム・サーバは、ローカル環境下のこれらクライアント端末をメンバー登録し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。勿論

、コンテンツを享受できる端末の台数に一定の制限を設ける必要がある。

#### 【0048】

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

#### 【0049】

一方、ホーム・ネットワーク上に存在しない、すなわちリモート環境のクライアント端末は、個人的又は家庭の範囲内での使用であるとは考えられない。リモート環境のクライアント端末にコンテンツの利用を認めると、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しくなるからである。そこで、ホーム・サーバは、リモート環境のクライアントをメンバーとして登録せず、また、コンテンツのライセンスを発行しない。

#### 【0050】

図1に示した例では、ホーム・ネットワーク上には1つのホーム・サーバしか存在しないが、勿論、2以上のホーム・サーバを同じホーム・サーバ上に設置して、各ホーム・サーバがホーム・ネットワーク内でそれぞれ独自にコンテンツの配信サービスを行なうようにしてもよい。

#### 【0051】

図2には、2台のホーム・サーバが存在するホーム・ネットワークの構成例を示している。

#### 【0052】

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

#### 【0053】

さらに、クライアント端末は、同じホーム・ネットワーク上の2台以上のホー

ム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。この場合も、クライアント端末は、それぞれのホーム・サーバにとってローカル環境下に存在し、個人的又は家庭の範囲内での使用であると推定されるから、ローカル環境内の各ホーム・サーバのコンテンツを自由に使用することが相当であると思料される。

#### 【0054】

一方、クライアント端末が複数のホーム・サーバに同時にメンバー登録できるからといって、複数のホーム・ネットワークに跨って複数のホーム・サーバのグループに所属することまでは認めるべきでない（図3を参照のこと）。

#### 【0055】

別のホーム・ネットワークに接続した時点で、元の接続先のホーム・ネットワークから見ればクライアント端末がリモート環境に移動したことに相当し、あるいは、あるホーム・ネットワークに接続した時点で他のホーム・ネットワークにとってクライアント端末はリモート環境に存在することに等しいからである。ローカル環境が個人的又は家庭の範囲内であるのに対し、リモート環境は個人的又は家庭の範囲を逸脱する。

#### 【0056】

クライアント端末が時間差をかけて複数のホーム・ネットワークに跨って接続することは技術的には可能であるが、これに併せてコンテンツの利用を逐次許可していくと、コンテンツの利用はほぼ無制限となってしまう、コンテンツに関する著作権は保護されないに等しくなる。

#### 【0057】

以上を総括すると、ホーム・ネットワーク上において、個人的又は家庭の範囲内での使用であると推定されるローカル環境を実現するためには、以下の事柄が必要条件であることが導出される。

#### 【0058】

(1) ホーム・サーバは、ホーム・ネットワーク外からのメンバー登録を認めない。

(2) 同じホーム・ネットワーク内に2台以上のホーム・サーバがあるときには、ホーム・サーバ毎にメンバー登録、グループ管理を行なう。ホーム・ネットワーク上の各クライアントは2以上のホーム・サーバに登録することができる。但し、同時登録されるホーム・サーバは同じホーム・ネットワークに存在しなければならない。

#### 【0059】

このようなローカル環境を実現するためには、ホーム・サーバとクライアント端末間で、お互い同じホーム・ネットワーク上に存在するかどうかを識別する仕組みが必要となる。

#### 【0060】

現状のネットワーク・プロトコルでは、ホーム・ネットワークなどネットワークをセグメント単位で識別する仕組みは提供されていない。そこで、本発明者らは、ホーム・ネットワークと外部ネットワークの間に介在するルータ又はゲートウェイにホーム・ネットワークを外部ネットワークから隔離する機能を装備し、例えばホーム・サーバがクライアントをメンバー登録したり、コンテンツの提供又はそのライセンスを発行したりするときに、ホーム・ネットワークを外部ネットワークから隔離又は遮断することによって、要求元クライアントがホーム・サーバと同じローカル環境に存在することを保証する、という方法を提案する。

#### 【0061】

図4には、本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示している。

#### 【0062】

家庭内に敷設されるホーム・ネットワークは、ホーム・ルータ経由でインターネットなどWAN、あるいは他のLANに接続されている。ホーム・ネットワークのdefault Gatewayはホーム・ルータに設定されている。

#### 【0063】

ホーム・ネットワークは、例えばハブ（集結装置）にホーム・サーバやクライアント端末などのホスト装置のLANケーブルを接続することにより構成される。

**【0064】**

ホーム・サーバやクライアント端末、ホーム・ルータなどのホーム・ネットワーク上のホスト装置、並びに外部ネットワーク上のホスト装置は、機器固有のMACアドレスを有している。ホスト装置は、受信先MACアドレス及び送信元MACアドレスを含んだヘッダ情報を持つパケット、例えばイーサネット（登録商標）フレームを、ネットワーク経由で送受信する。

**【0065】**

ホーム・サーバやクライアント端末などのホーム・ネットワーク上のホスト装置は、例えばUPnP対応機器として構成される。この場合、ネットワークに対する接続機器の追加や削除が容易である。ホーム・ネットワークに新たに接続する機器は、以下の手順に従って、コンテンツ利用などホーム・ネットワーク上のサービスを享受することができるようになる。

**【0066】**

- (1) アドレッシング処理：IPアドレスなどの自己のデバイスIDを取得する
- (2) ディスカバリ処理：ネットワーク上の各デバイスの検索を行ない、各デバイスから受信した応答に含まれるデバイス種別や機能などの情報を取得する
- (3) サービス要求処理：ディスカバリ処理で取得された情報に基づいて各デバイスにサービスを要求する

**【0067】**

ホーム・ネットワーク上では、個人的又は家庭の範囲内での使用であると推定されるローカル環境が形成されている。したがって、ホーム・サーバは、ホーム・ルータ経由で外部ネットワーク上のコンテンツ・サーバから正当にコンテンツを取得し、蓄積し、家庭内でコンテンツを配信する。また、各クライアント端末は、ホーム・サーバに所望のコンテンツを要求し、これを取得して利用することが許容される。

**【0068】**

ローカル環境下では、クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。

## 【0069】

また、図5には、本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示している。

## 【0070】

ホーム・ネットワークは、ホーム・ルータ経由でインターネットなどWAN、あるいは他のLANに接続されている。この場合も、ホーム・ネットワークの default Gatewayはホーム・ルータに設定されている。

## 【0071】

図4との相違は、ホーム・ネットワーク上に2台のホーム・サーバが存在する点である。各ホーム・サーバは、ホーム・ネットワーク上に同時に存在してもよいし、あるいは時間差を以って接続されてもよい。

## 【0072】

この場合、各ホーム・サーバは、同じホーム・ネットワーク上のクライアント端末はローカル環境下にあることから、これらをメンバー登録してグループを形成し、コンテンツ配信並びにコンテンツ使用のライセンスを発行する。クライアント端末は、ホーム・サーバからコンテンツを取得し、コピーやストリーミングなどコンテンツを利用し、さらにローカル環境外（リモート環境）にコンテンツを持ち出して利用することができる。また、クライアント端末は、同じホーム・ネットワーク上の2台以上のホーム・サーバに対し同時にメンバー登録し複数のグループに所属し、各々のホーム・サーバからコンテンツのライセンスを取得することができる。

## 【0073】

図6には、サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示している。

## 【0074】

このシステムは、プロセッサ10を中心に構成されている。プロセッサ10は、メモリに記憶されたプログラムに基づいて各種の処理を実行する。また、プロセッサは、バス30を介して接続されている各種の周辺機器を制御している。バス30に接続された周辺機器は次のようなものである。

**【0075】**

メモリ20は、例えばDRAM (Dynamic RAM) などの半導体メモリで構成され、プロセッサ10において実行されるプログラム・コードをロードしたり、実行プログラムの作業データを一時格納したりするために使用される。

**【0076】**

ディスプレイ・コントローラ21は、プロセッサ10から送られてくる描画命令に従って表示画像を生成し、表示装置22に送る。ディスプレイ・コントローラに接続された表示装置22は、ディスプレイ・コントローラ21から送られた表示画像情報に従い、その画像を画面に表示出力する。

**【0077】**

入出力インターフェース23は、キーボード24やマウス25が接続されており、キーボード24やマウス25からの入力信号をバス30経由でプロセッサ10へ転送する。

**【0078】**

ネットワーク・インターフェース26は、ホーム・ネットワーク (ハブ) に接続され、さらにホーム・ルータ40経由でインターネットなどの外部ネットワークに接続されており、インターネットを介したデータ通信を制御する。すなわち、プロセッサ10から送られたデータをインターネット上の他の装置へ転送するとともに、インターネットを介して送られてきたデータを受け取りプロセッサ10に渡す。

**【0079】**

ハード・ディスク装置 (HDD: Hard Disk Drive) コントローラ27には、HDDなどの大容量外部記憶装置28が接続されており、HDDコントローラ27が接続されたHDD28へのデータの入出力を制御する。HDD28には、プロセッサが実行すべきオペレーティング・システム (OS) のプログラム、アプリケーション・プログラム、ドライバ・プログラムなどが格納されている。アプリケーション・プログラムは、例えば、ホーム・サーバとしてホーム・ネットワーク上の各クライアント端末の認証処理を行ったり、コンテンツの提供やライセンスの発行を行ったりするサーバ・アプリケーションや、サ

サーバから提供されたコンテンツの再生などコンテンツの利用を行なうクライアント・アプリケーションなどである。

#### 【0080】

なお、ホスト装置を構成するためには、図6に示した以外にも多くの電気回路などが必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。また、図面の錯綜を回避するため、図中の各ハードウェア・ブロック間の接続も一部しか図示していない点を了承されたい。

#### 【0081】

図7には、ホーム・ネットワークと外部ネットワークを接続するホーム・ルータ40の内部構造を示している。LAN通信部41は、ホーム・サーバとの通信を行なうための送受信機能である。遮断器42は、ホーム・ネットワークをWANなどの外部ネットワークと隔離又は遮断する機能モジュールである。制御部43は、LAN通信部41を通じた通信をコントロールし、ホーム・サーバとの認証の実施や、制御メッセージの交換、遮断器42の制御などを行なう。記憶部44は、制御部43の動作プログラムやそのために必要なデータ、認証のための鍵情報などを蓄積する。

#### 【0082】

また、図8には、ホーム・ルータ40の別の実装形態を示している。同図に示す構成では、遮断器42で外部ネットワークとホーム・ネットワークを切り離した状態でも、ホーム・ルータ40はWAN通信部45によって外部ネットワークとの通信が可能である。この場合、例えば、他に外部ネットワークと通信している装置が存在しないかを監視したり、さらに別の装置、例えば別のモデムに対して外部ネットワークとの経路遮断を指示したり、その指示通りに通信が遮断されているかを、実際に外部ネットワーク上の所定のサーバへのアクセスを試すことで確認するといったことをWAN通信部45を利用して行なうことで、より確実に遮断を実現することができる。

#### 【0083】

図9には、ホーム・ルータ40によるホーム・ネットワークと外部ネットワー

クとの経路遮断を行なうための処理手順を示している。

#### 【0084】

ホーム・サーバは、クライアント端末をホーム・ネットワーク内のグループのメンバーとして登録したり、私的にのみ利用可能なコンテンツ又はそのライセンスをクライアント端末に提供したりする段階で、クライアント端末がローカル環境すなわち同じホーム・ネットワーク上に存在することを確保しなければならない。

#### 【0085】

このようにローカルな通信が必要になった段階で、ホーム・サーバはホーム・ルータ40に対し、外部ネットワークへの経路の遮断を依頼する。

#### 【0086】

経路遮断に先立って、ホーム・ルータ40が依頼通りに働く正当な機器であることを確認するため、認証処理を行なうようにしてもよい。但し、一般のUPnP対応ルータのように、遮断の制御はできても認証機能は持たないケースもあり得るので、認証処理は必須ではない。

#### 【0087】

この認証には、例えば、一般的なチャレンジ・レスポンス認証などが適用される。この場合、ホーム・サーバから乱数をホーム・ルータ40に送り、これに対し、ホーム・ルータ40はホーム・サーバと共有する秘密鍵を乱数に連結してハッシュ化したものを求め、ホーム・サーバに返送する。ホーム・サーバは、同様の方法でホーム・ルータ40が返送してくる筈の期待値を求め、一致が確認されれば認証を成功とする。このような共有秘密鍵ベースの方法の他に、公開鍵ベースの、ホーム・ルータ40の秘密鍵で暗号化して返送するという方法もある。

#### 【0088】

認証成功後は、ホーム・サーバからホーム・ルータ40に経路の遮断を指示する。このようにして、ホーム・ネットワークが外部ネットワークから隔離又は遮断された状態で、ホーム・サーバはクライアント端末をホーム・ネットワーク内のグループのメンバーとして登録したり、私的にのみ利用可能なコンテンツ又はそのライセンスをクライアント端末に提供したりするなどのローカル通信を行な

う。

#### 【0089】

クライアント端末は、ホーム・サーバと同じローカル環境に存在する場合にのみ、メンバー登録やコンテンツ又はそのライセンスの提供を受けることができ、外部ネットワークからのなりすましを防止することができる。ローカル環境内においてのみ機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

#### 【0090】

その後、ホーム・サーバからホーム・ルータに経路の再開を指示することによって、ホーム・ネットワークと外部ネットワーク間を遮断した経路を復活させる。

#### 【0091】

但し、ローカル通信を行なう期間中ホーム・ネットワークを外部ネットワークから遮断する必要はない。例えば、ローカル通信を開始してから所定時間だけホーム・ネットワークを外部ネットワークから隔離することによっても、クライアント端末がローカル環境に存在することを保証することができる。したがって、ホーム・ネットワークと外部ネットワーク間の経路の再開は、ホーム・ルータ40がホーム・サーバからの指示（コマンド）に応答して行なうのではなく、経路を遮断してから所定時間経過後に自律的に経路の再開を行なうように構成してもよい。

#### 【0092】

なお、認証成功後の上記制御についても、第3者によるなりすましを防ぐため、認証を通じて鍵を共有し、その鍵で制御通信を保護するという方法もある。例えば、前記ハッシュ化した結果を、認証に使う部分と鍵として使う部分に分けて、鍵は制御通信のメッセージのハッシュ化に使う。そして、このハッシュ化の結果を制御メッセージとともに送ることで、受信した装置における同様のハッシュ処理によるメッセージの正当性チェックが可能である。

#### 【0093】

また、図9に示した動作シーケンス例では、ホーム・ルータ40は、ホーム・

サーバからの明示的な指示（自身宛のコマンド）に応答して、ホーム・ネットワークと外部ネットワーク間の経路の遮断を実行するようになっているが、ホーム・ルータ40が自律的に経路の遮断を行なうように構成することもできる。例えば、ホーム・ルータ40は、LAN通信部41を通じてホーム・ネットワーク上の動作（すなわち、ネットワーク上の転送コマンド）を常時監視し、ホーム・サーバがクライアント端末をホーム・ネットワーク内のグループのメンバーとして登録したり、私的にのみ利用可能なコンテンツ又はそのライセンスをクライアント端末に提供したりするなどのローカル通信を行なうタイミングを検出し、このようなタイミングにおいて自律的に経路の遮断動作を起動する。この場合、勿論、ホーム・ルータ40が自律的に経路の再開を行なうように構成してもよい。

#### 【0094】

##### [追補]

以上、特定の実施形態を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施形態の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、本明細書の記載内容を限定的に解釈するべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

#### 【0095】

##### 【発明の効果】

以上詳記したように、本発明によれば、ルータ経由で外部ネットワークに接続されているホーム・ネットワーク上でコンテンツの利用を好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することができる。

#### 【0096】

また、本発明によれば、ホーム・ネットワーク上の各クライアント端末がホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内で利用するように好適に管理することができる、優れた機器間認証システム及び機器間認証方法、通信機器、並びにコンピュータ・プログラムを提供することができる。

**【0097】**

本発明によれば、ローカル環境内においてのみ機器間でコンテンツの利用を認めることにより、コンテンツの不正流通を効果的に抑制することができる。

**【図面の簡単な説明】****【図1】**

ホーム・ネットワークの基本構成を模式的に示した図である。

**【図2】**

2台のホーム・サーバが存在するホーム・ネットワークの構成例を示した図である。

**【図3】**

クライアント端末が複数のホーム・ネットワークに跨って接続する様子を示した図である。

**【図4】**

本発明の一実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

**【図5】**

本発明の他の実施形態に係るホーム・ネットワークの構成を模式的に示した図である。

**【図6】**

サーバやクライアントなどとしてホーム・ネットワークに接続されるホスト装置のハードウェア構成を模式的に示した図である。

**【図7】**

ホーム・ネットワークと外部ネットワークを接続するホーム・ルータ40の内部構造を示した図である。

**【図8】**

ホーム・ネットワークと外部ネットワークを接続するホーム・ルータ40の内部構造についての他の実現例を示した図である。

**【図9】**

ホーム・ルータ40によるホーム・ネットワークと外部ネットワークとの経路

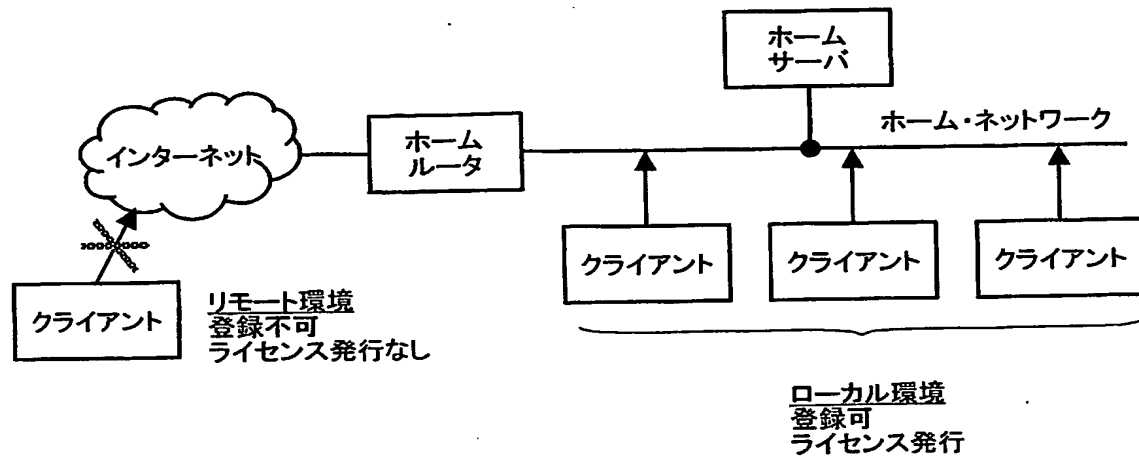
遮断を行なうための処理手順を示した動作シーケンス図である。

【符号の説明】

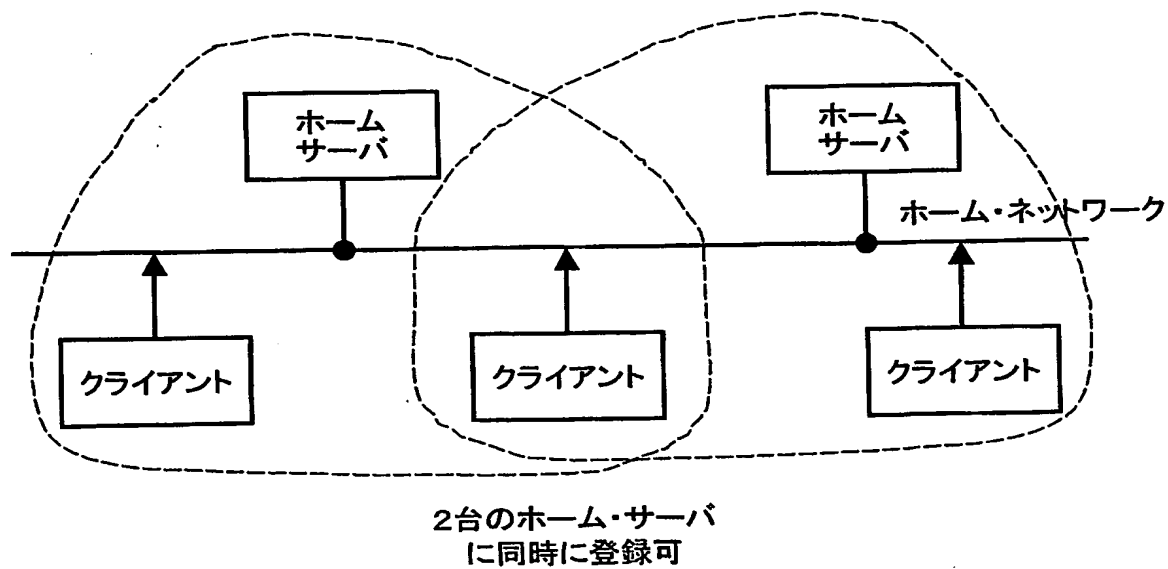
- 10…プロセッサ
- 20…メモリ
- 21…ディスプレイ・コントローラ
- 22…表示装置
- 23…入出力インターフェース
- 24…キーボード
- 25…マウス
- 26…ネットワーク・インターフェース
- 27…ハード・ディスク装置コントローラ
- 28…HDD
- 30…バス
- 40…ホーム・ルータ
- 41…LAN通信部
- 42…遮断器
- 43…制御部
- 44…記憶部

【書類名】 図面

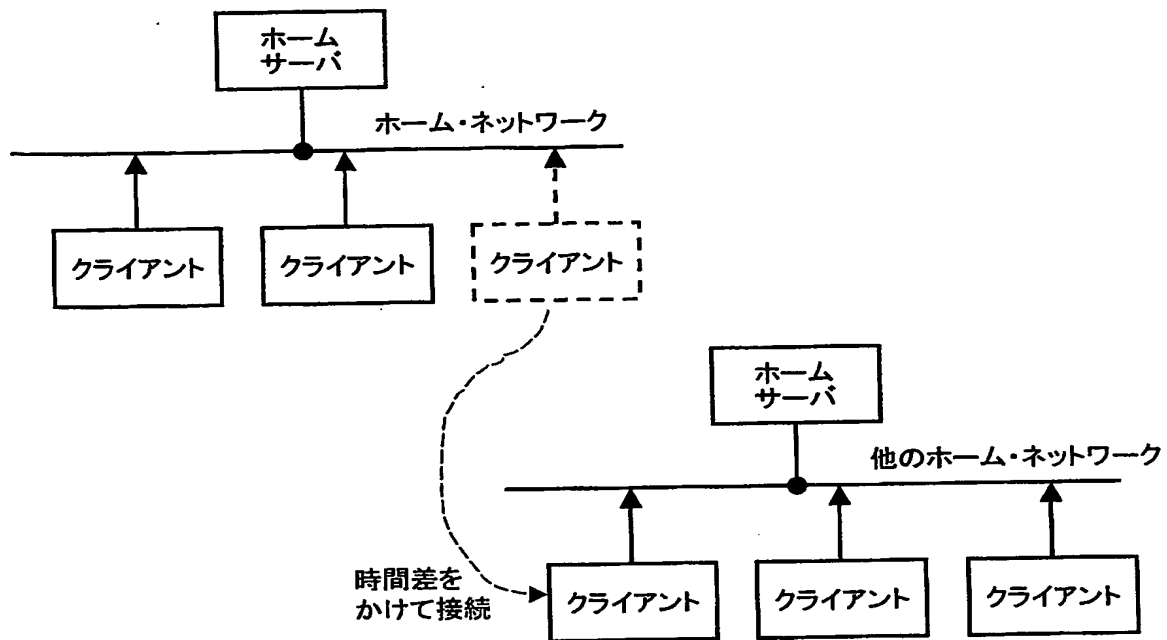
【図 1】



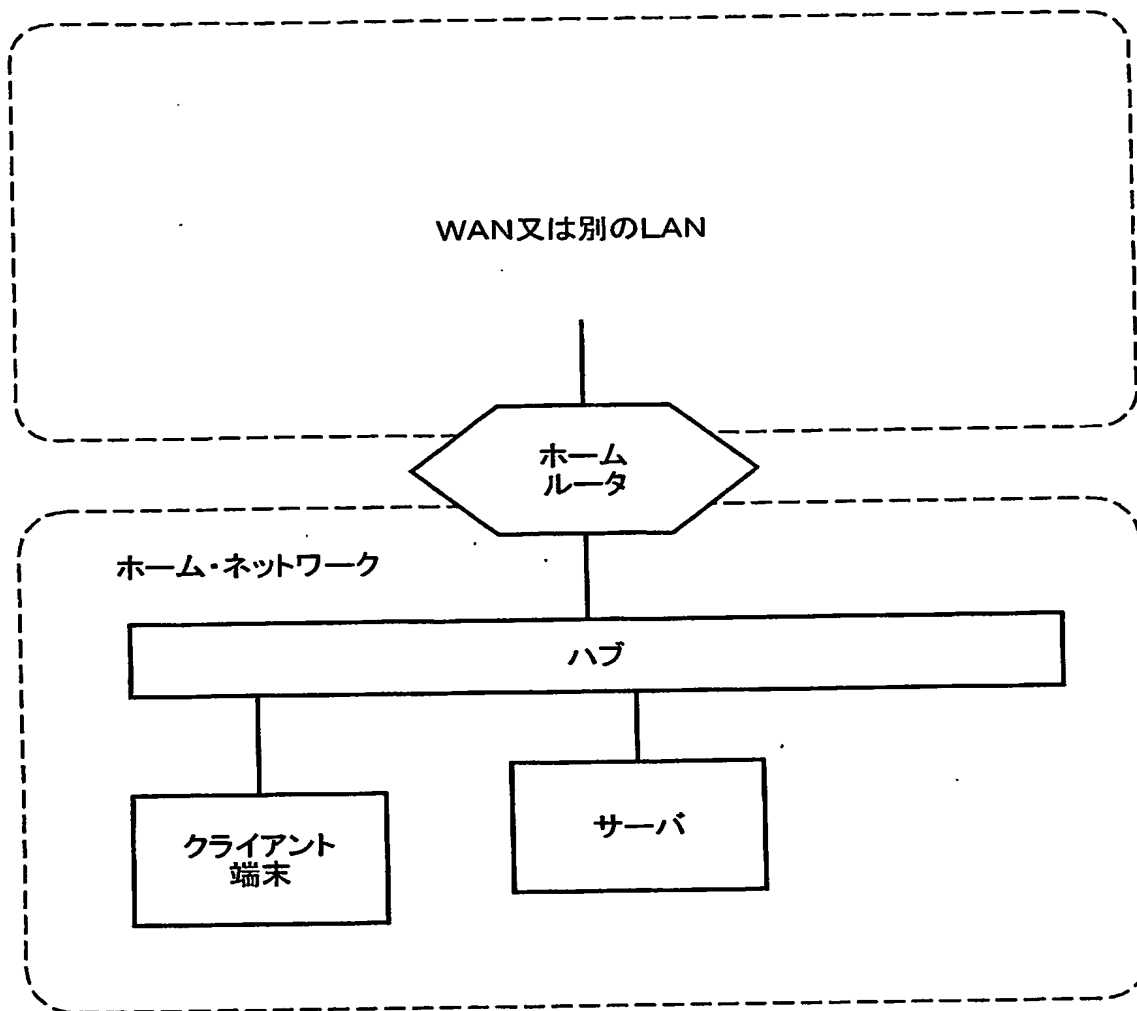
【図 2】



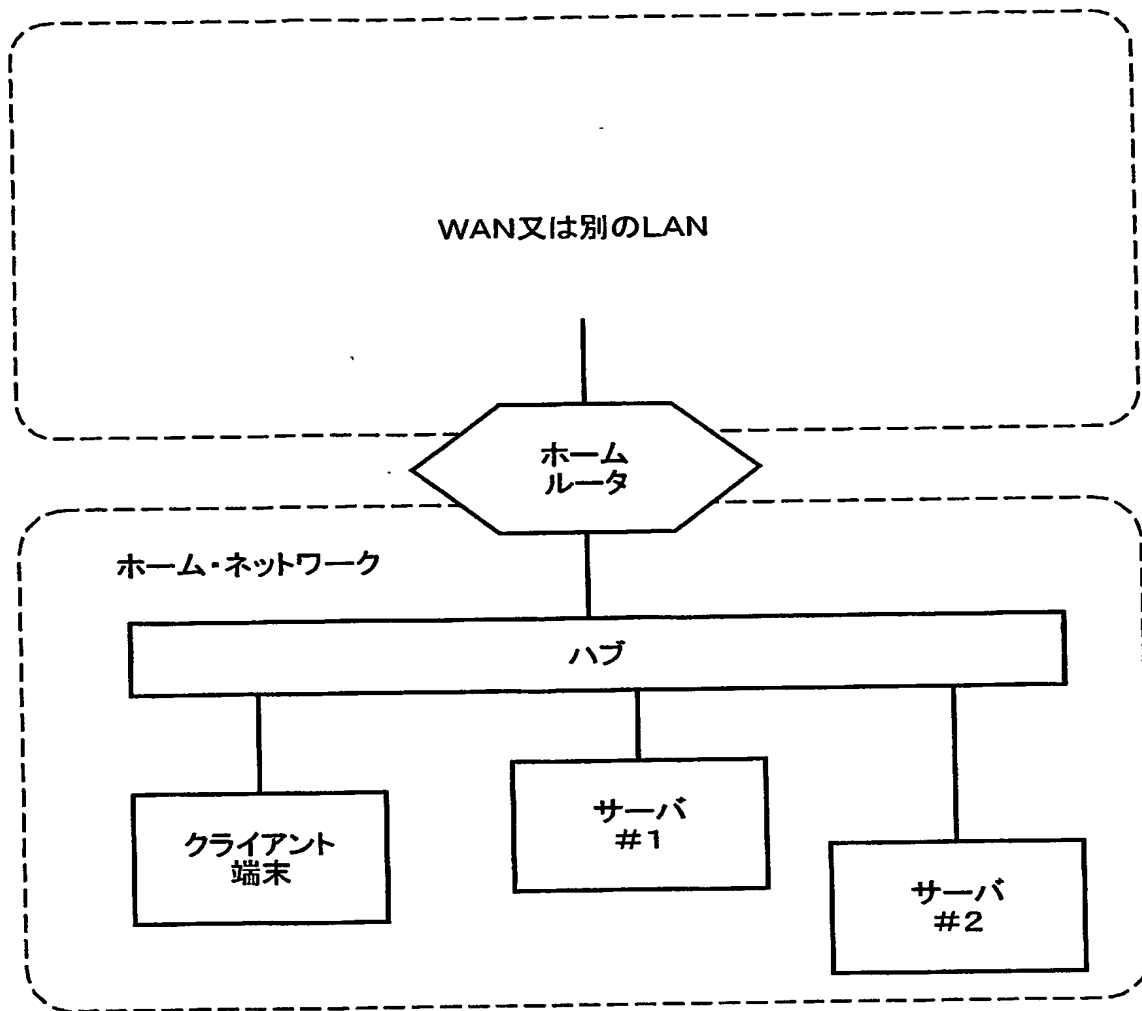
【図 3】



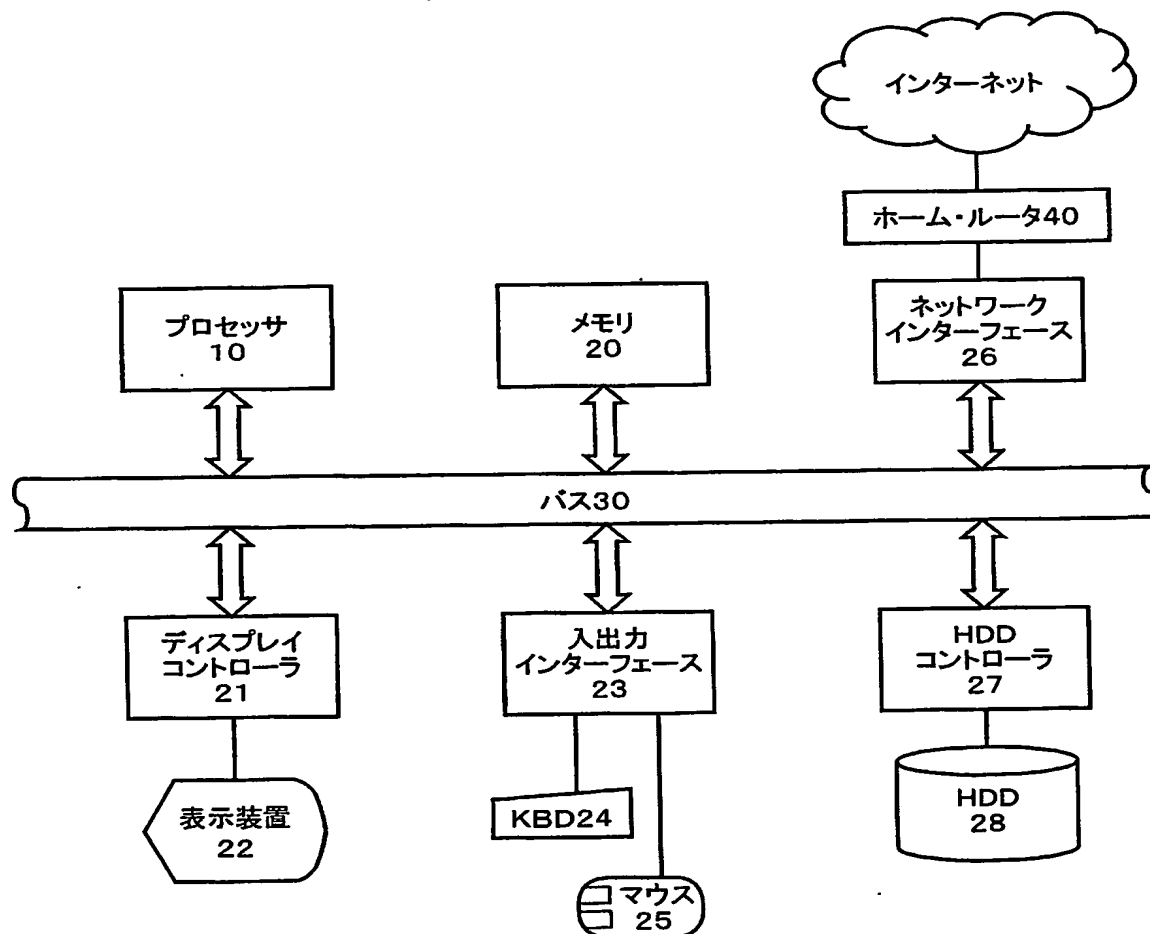
【図4】



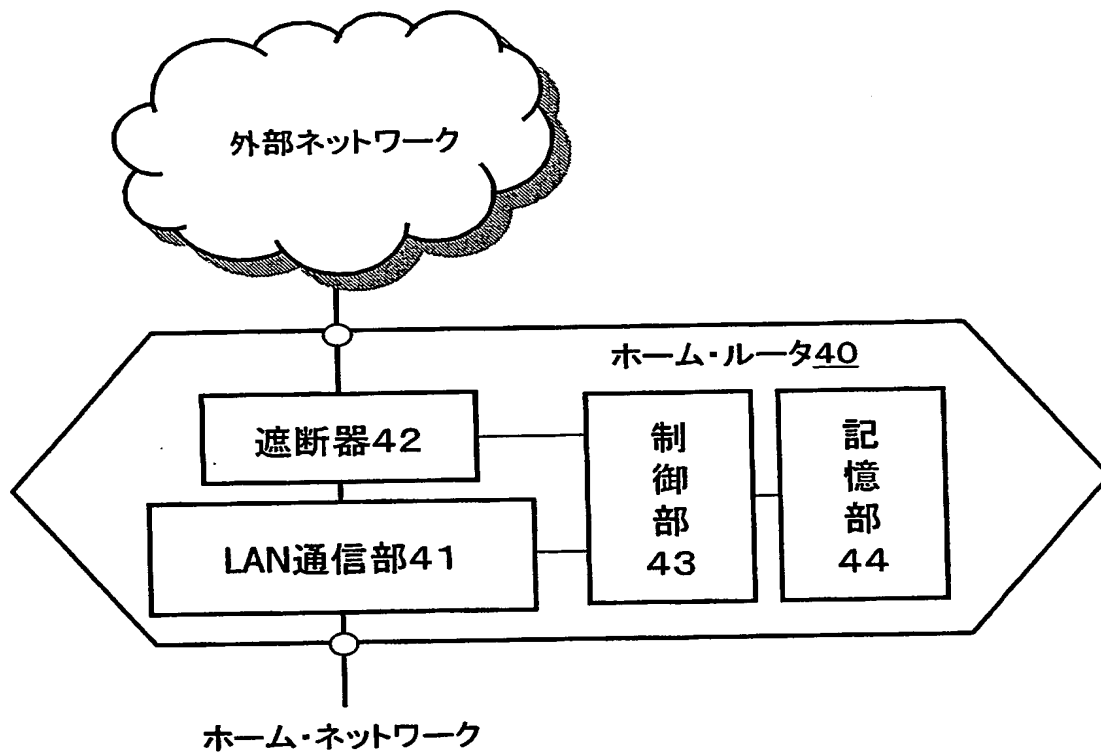
【図5】



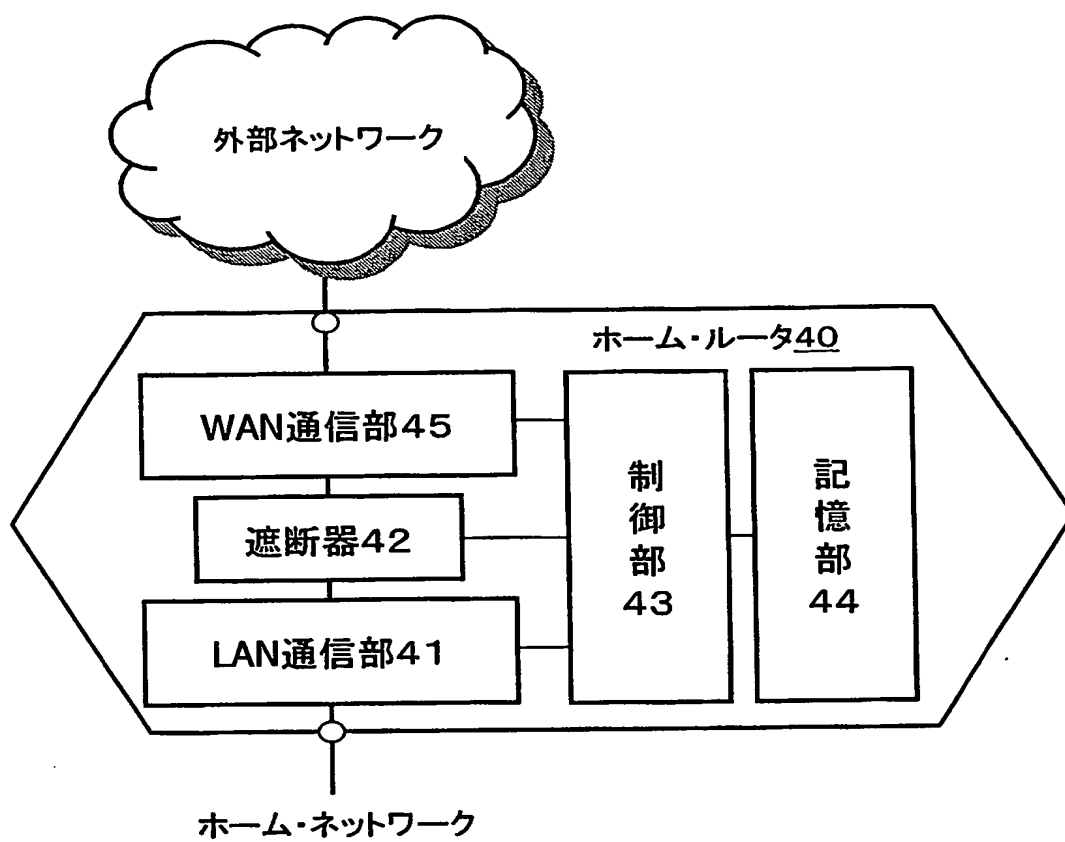
【図6】



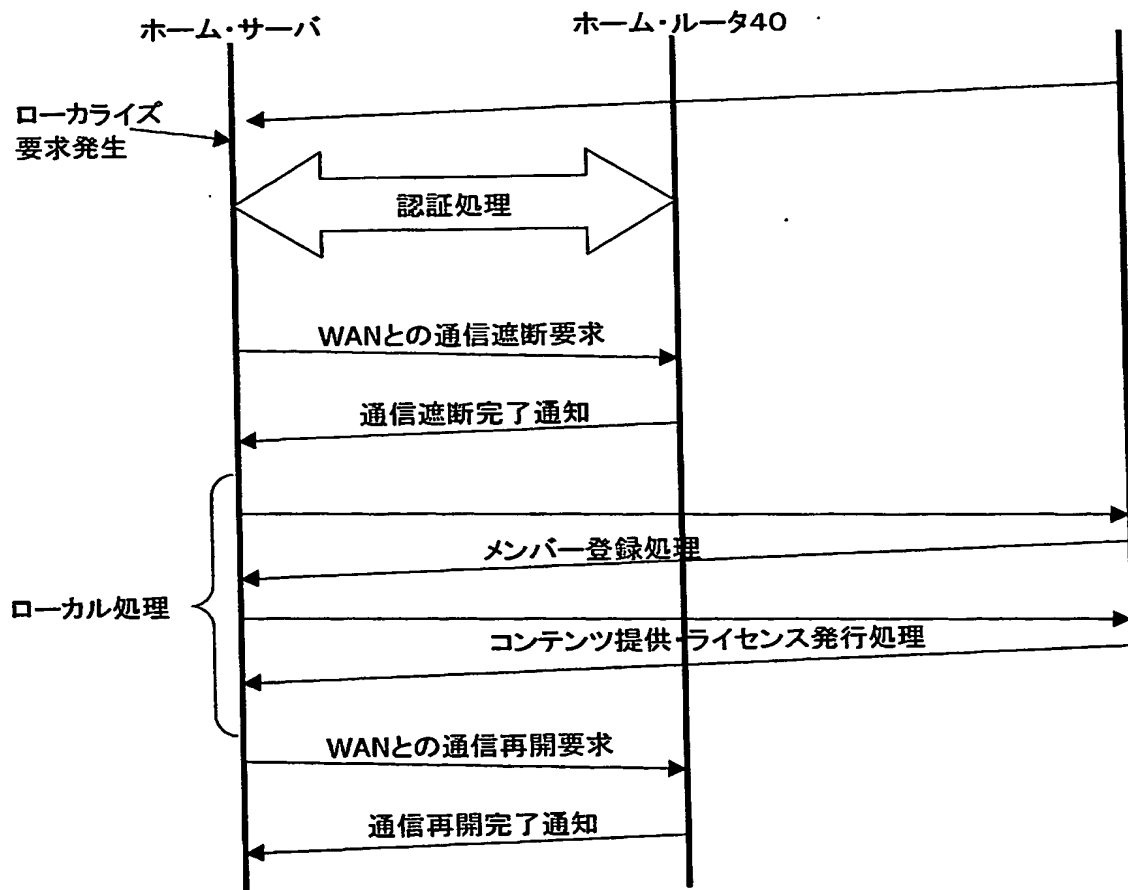
【図7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】 ホーム・サーバ上で正当に取得されているコンテンツを著作権法で認められる私的使用の範囲内でクライアント端末が利用するように管理する。

【解決手段】 ホーム・ネットワークと外部ネットワークの間に介在するルータ又はゲートウェイにホーム・ネットワークを外部ネットワークから隔離する機能を装備し、例えばホーム・サーバがクライアントをメンバー登録したり、コンテンツの提供又はそのライセンスを発行したりするときに、ホーム・ネットワークを外部ネットワークから隔離することによって、要求元クライアントがローカル環境に存在することを保証する。

【選択図】 図 1

特願 2 0 0 3 - 1 3 2 9 0 4

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日  
[変更理由]

住 所  
氏 名

1 9 9 0 年 8 月 3 0 日  
新規登録  
東京都品川区北品川 6 丁目 7 番 3 5 号  
ソニー株式会社